(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 532 226 A3**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **92307998.2**

(51) Int. Cl.[5] : **H04L 9/08,** H04L 9/32

(22) Date of filing : **03.09.92**

(30) Priority : **13.09.91 US 759312**

(43) Date of publication of application :
17.03.93 Bulletin 93/11

(84) Designated Contracting States :
DE FR GB SE

(88) Date of deferred publication of search report :
13.04.94 Bulletin 94/15

(71) Applicant : **AMERICAN TELEPHONE AND TELEGRAPH COMPANY**
32 Avenue of the Americas
New York, NY 10013-2412 (US)

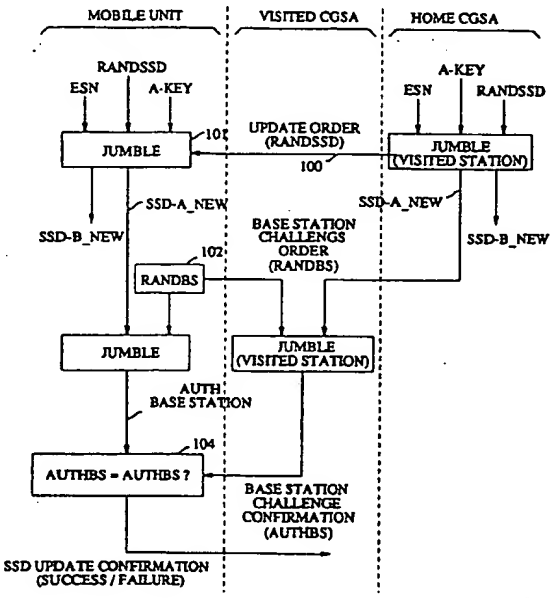
(72) Inventor : **Reeds III, James Alexander**
127 Southgate Road
New Providence, New Jersey 07974 (US)
Inventor : **Treventi, Philip Andrew**
15 Candlewood Drive
Murray Hill, New Jersey 07974 (US)

(74) Representative : **Buckley, Christopher Simon Thirsk et al**
AT & T (UK) LTD., AT & T Intellectual Property Division, 5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) Speech and control message encryption in cellular radio.

(57) A protocol for authenticating a mobile customer unit to a service provider where signaling messages are encrypted and where voice communications can be encrypted. A service provider assigns to each mobile customer unit a unique "secret", along with other information such as a telephone number. At the pleasure of the service provider, a directive is sent to the mobile customer unit to create a shared secret datum based on the secret. The shared secret datum is created with the aid of a bit string that is sent for that purpose by the provider. A portion of the created shared secret datum is used for encrypting speech and the same or other portion of the created shared secret datum is used as an input to a process for creating a second encryption key. That key is employed in the mobile customer unit to encode those of the control signals generated by the mobile customer unit that affect the nature of the call in progress.

FIG. 3



EP 0 532 226 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 92 30 7998

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
Y	EP-A-0 354 770 (IBM) * column 6, line 43 - line 61 * * column 10, line 57 - column 11, line 12 * * column 18, line 52 - column 19, line 6 * * column 21, line 56 - column 22, line 10 * ---	1,2,5,6	H04L9/08 H04L9/32
Y	EP-A-0 105 553 (STAAT DER NEDERLANDEN) * page 4, line 11 - line 20 * ---	1,2,5,6	
A	AT & T BELL LABORATORIES TECHNICAL JOURNAL vol. 63, no. 8 , October 1984 , NEW YORK US pages 1673 - 1683 J. REEDS ET AL 'FILE SECURITY AND THE UNIX SYSTEM CRYPT COMMAND' * page 1674, line 22 - page 1675, line 9 * ---	1,2,5,6	
A	WO-A-84 00656 (TELEASE) * page 7, line 16 - line 23 * * page 16, line 18 - line 27 * * page 28, line 25 - line 29 * -----	3,4,7,8	

TECHNICAL FIELDS SEARCHED (Int.Cl.5)

H04L
H04K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	14 February 1994	Holper, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)